CORE
Metadata, citation and similar papers at core.ac.uk
Provided by Electronic Theses and Dissertations at Indian Institute of Science

Abstract

There has been a rapid increase of interest in computational number theory ever since the invention of public-key cryptography. Various attempts to solve the underlying hard problems behind public-key cryptosystems has led to interesting problems in computational number theory. One such problem, called the cubic sieve congruence problem, arises in the context of the cubic sieve method for solving the discrete logarithm problem in prime fields.

The cubic sieve method requires a nontrivial solution to the Cubic Sieve Congruence (CSC) $x^3 \equiv y^2 z \pmod{p}$, where p is a given prime. A nontrivial solution must satisfy

$$x^3 \equiv y^2 z \pmod{p}, \quad x^3 \neq y^2 z, \quad 1 \leq x\,, y,\, z < p^{\alpha},$$

where α is a given real number and $\frac{1}{3} < \alpha \leq \frac{1}{2}$. The CSC problem is to find an efficient algorithm to obtain a nontrivial solution to CSC.

This thesis is concerned with the CSC problem. Recently, the parametrization $x \equiv v^2 z \pmod{p}$ and $y \equiv v^3 z \pmod{p}$ of CSC was introduced. We give a deterministic polynomial-time ($O(\ln^3 p)$ bit-operations) algorithm to determine, for a given v, a nontrivial solution to CSC, if one exists. Previously it took $\widetilde{O}(p^{\alpha})$ time to do this. We relate the CSC problem to the gap problem of fractional part sequences. We also show in the $\alpha = \frac{1}{2}$ case that for a certain class of primes the CSC problem can be solved deterministically in $\widetilde{O}\left(p^{\frac{1}{3}}\right)$ time compared to the previous best of $\widetilde{O}\left(p^{\frac{1}{2}}\right)$. It is empirically observed that about one out of three primes are covered by this class, up to 10^9.